IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	Confirmation No.: 3428
Michael Frederick KENRICH	Art Unit: 2434
Application No.: 10/690,243	Examiner: Farid HOMAYOUNMEHR
Filed: October 20, 2003	Atty. Docket: 2222.5460000
For: **Method and System for Proxy Approval of Security Changes for a File Security System**	

Brief on Appeal Under 37 C.F.R. § 41.37

Mail Stop Appeal Brief - Patents

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

A Notice of Appeal from the final rejection of claims 1-16, 18-38 and 45-51 is filed concurrently. Appellant hereby files one copy of this Appeal Brief, together with the required fee set forth in 37 C.F.R. § 41.20(b)(2).

It is not believed that extensions of time are required beyond those that may otherwise be provided for in documents accompanying this paper. However, if additional extensions of time are necessary to prevent abandonment of this application, then such extensions of time are hereby petitioned under 37 C.F.R. § 1.136(a), and any fees required therefor (including fees for net addition of claims) are hereby authorized to be charged to our Deposit Account No. 19-0036.

Table of Contents

I. Real Party In Interest (37 C.F.R. § 41.37(c)(1)(i))

The real party in interest in this appeal is PSS Systems, Inc., the assignee of record.

II. Related Appeals and Interferences (37 C.F.R. § 41.37(c)(1)(ii))

No other prior and pending appeals, interferences or judicial proceedings are known to appellant, the appellant's legal representative, or assignee which may be related to, directly affect or be directly affected by or have a bearing on a decision by the Board of Patent Appeals and Interferences ("the Board") in the pending appeal.

III. Status of Claims (37 C.F.R. § 41.37(c)(1)(iii))

Claims 1-33 were filed on October 20, 2003 at initial filing of the instant Application.

An Office Action was mailed on July 16, 2007 ("Office Action 1") in which claims 1-33 were rejected. An Amendment and Reply Under 37 C.F.R. § 1.111 responsive to the Office Action 1 was filed October 16, 2007 ("Reply to Office Action 1") amending claims 1-16 and 18-36 and adding new claims 34-36. Claim 17 was cancelled.

A Final Office Action was mailed January 8, 2008 ("Final Office Action 1") in which claims 1-16 and 18-36 were finally rejected. A Reply Under 37 C.F.R. § 1.116 responsive to the Final Office Action 1 was filed April 23, 2008 ("Reply to Final Office Action 1") amending claims 1, 15, 30 and 34-36. An Advisory Action was mailed on May 16, 2008 ("Advisory Action 1") maintaining the rejections. A Request for Continued Examination ("RCE 1") was filed on May 18, 2008.

An Office Action was mailed on August 20, 2008 ("Office Action 2") in which claims 1-16 and 18-36 were rejected. A Reply Under 37 C.F.R. § 1.111 responsive to the Office Action 2 was filed November 20, 2008 ("Reply to Office Action 2") in which no claims were amended.

A Final Office Action was mailed on February 20, 2009 ("Final Office Action 2") in which claims 1-16 and 18-36 were rejected. A Reply Under 37 C.F.R. § 1.116 responsive to the Final Office Action 2 was filed April 20, 2009 ("Reply to Final Office Action 2") in which no claims were amended. An Advisory Action ("Advisory Action 2") maintaining

the rejections was mailed on April 27, 2009. A Notice of Appeal ("Notice of Appeal 1") and a Pre-Appeal Conference Request were filed on May 13, 2009 appealing the final rejection of claims 1-16 and 18-36. A Pre-Appeal Conference decision ("Panel Decision") was mailed on July 20, 2009 indicating that the application remained under appeal. A Request for Continued Examination ("RCE 2") and Amendment and Reply Under 37 C.F.R. § 1.116 ("Second Reply to Final Office Action 2") responsive to the Final Office Action 2, Advisory Action 2 and Panel Decision was filed on August 19, 2009 in which claims 1, 15, 30, 34, 35 and 36 were amended and new claims 37 and 38 were added.

An Office Action was mailed October 27, 2009 ("Office Action 3") in which claims 1-16 and 18-38 were rejected. A Reply Under 37 C.F.R. § 1.111 responsive to the Office Action 3 was filed January 27, 2010 ("Reply to Office Action 3") in which the specification and claims 1, 3-11, 14-16, 18-24 and 26-38 were amended and new claims 39-48 were added.

A Final Office Action was mailed May 6, 2010 ("Final Office Action 3") in which claims 1-16 and 18-48 were rejected. A Reply Under 37 C.F.R. § 1.116 responsive to the Final Office Action 3 was filed July 6, 2010 ("Reply to Final Office Action 3") in which claims 1, 15, 30, 34-36 and 39-44 were amended. An Advisory Action ("Advisory Action 2") maintaining the rejections was mailed on July 16, 2010. A Request for Continued Examination ("RCE 3") was filed on August 5, 2010 to request the entry of Reply to Final Office Action 3.

A Notice of Allowance was mailed September 29, 2010 in which claims 1-16, 18-38 and 45-48 were allowed. A Request for Continued Examination ("RCE 4"), Information

Disclosure Statement and Preliminary Amendment Under 37 C.F.R. § 1.115 were filed November 19, 2010 in which the specification was amended and new claims 49-51 were added.

An Office Action ("Office Action 4") was mailed January 18, 2011 in which claims 1-16, 18-38 and 45-51 were rejected. A Reply Under 37 C.F.R. § 1.111 responsive to the Office Action 4 was filed May 18, 2011 ("Reply to Office Action 4") in which the specification and claim 49 were amended.

A Final Office Action ("Final Office Action 4") was mailed August 1, 2011 in which claims 1-16, 18-38 and 45-51 were rejected. A Notice of Appeal ("Notice of Appeal 2") is filed concurrently herewith from the Final Office Action, from which this Brief on Appeal follows. Claims 1-16, 18-38 and 45-51 are pending, finally rejected, and are the subject of this Appeal. A copy of the claims on appeal can be found in the attached Claims Appendix as required under 37 C.F.R. § 41.37(c)(1)(viii).

IV. Status of Amendments (37 C.F.R. § 41.37(c)(1)(iv))

No amendments were sought to be made subsequent to the Final Office Action dated August 1, 2011.

V. Summary of Claimed Subject Matter (37 C.F.R. § 41.37(c)(1)(v))

A concise explanation of the invention is provided below for each of the independent claims involved in the appeal. The explanation refers to the specification by page and line number, and to the drawings, if any, by reference characters.

For each independent claim involved in the appeal and for each dependent claim argued separately under the provisions of paragraph (c)(1)(vii), every means plus function and step plus function as permitted by 35 U.S.C. § 112, sixth paragraph, are identified. The structure, material, or acts described in the specification as corresponding to each claimed function are set forth with reference to the specification by page and line number, and to the drawings, if any, by reference characters.

A. Independent Claim 1

Claim 1 recites a method for approving a security change for a file security system that secures electronic files **(see, e.g., p. 4, paragraph [0012], FIG. 3)**, comprising:

- receiving a request for the security change from a requestor **(see, e.g., p. 9, paragraph [0036], FIG. 3, element 302)**, the security change being used for determining access rights comprising permission to retrieve and to receive an electronic file from within a secure file store **(see, e.g., p. 7-8, paragraphs [0032] and [0033], element 204)**;
- identifying a plurality of approvers to approve or disapprove of the requested security change **(see, e.g., p. 9, paragraph [0036], FIG. 3, element 304)** by accessing an approver set in an approval manager module **(see, e.g. p. 11-12, paragraphs [0044] and [0045], FIGs. 2 and 5A, elements 208 and 502)**;
- notifying the approvers of an approval request for the requested security to change **(see, e.g., p. 9, paragraph [0036], FIG. 3 and 5A, element 306 and 506)**;
- determining, for at least one response received from the approvers, whether it remains possible for a quorum of the approvers to approve the requested security change **(see, e.g. p. 13, paragraph [0049], FIG. 5A, element 514)**; and

- determining whether the requested security change is approved based on responses from the approvers to the approval request **(see, e.g. p. 13, paragraph [0049], FIG. 5A, elements 514, 516 and 518)**.

B. Independent Claim 15

Claim 15 recites a file security system configured to restrict access to secured electronic documents **(see, e.g. p. 7-8, paragraph [0032], FIG. 2, element 200)**, comprising:

- an access server device configured to restrict access to the secured electronic documents **(see, e.g., p. 8, paragraph [0032], FIG. 2, element 202)**; and
- an approval manager operatively connected to said access server and configured to operate a security change approval process to determine whether a requested security change is approved **(see, e.g., p. 8, paragraph [0033], FIG. 2, element 208)**, the security change being used for determining access rights comprising permission to retrieve and to receive the secured electronic documents from within a secure file store **(see, e.g., p. 8, paragraph [0033], FIG. 2, element 204)**,
- wherein, in operating the security change approval process, the approval manager is configured to notify a plurality of approvers of the requested security change, to ask the approvers to approve or disapprove the requested security change, and to access an approver set to identify the plurality of approvers **(see, e.g., p. 12, paragraphs [0045]-[0047], FIG. 5A, elements 502 and 506)**, and
- wherein the approval manager is further configured to determine, for at least one response received from the approvers, whether it remains possible for a quorum of the approvers to approve the requested security change **(see, e.g., p. 13, paragraph [0049], FIG. 5A, element 514)**.

C. Independent Claim 30

Claim 30 recites an article of manufacture including a computer-readable storage medium having stored thereon computer-executable instructions, execution of which, by a computing device **(see, e.g., p. 17, paragraph [0066])**, causes the computing device to perform operations for approving a security change for a file security system that secures electronic files **(see, e.g., p. 4, paragraph [0012], FIG. 3)**, the operations comprising:

- notifying a plurality of approvers of an approval request for the requested security change **(see, e.g., p. 12, paragraph [0047], FIG. 5A, element 506)**, the plurality of approvers identified by accessing an approver set in an approval manager module **(see, e.g. p. 11-12, paragraphs [0044] and [0045], FIGs. 2 and 5A, elements 208 and 502)**;

- determining, for at least one response received from the approvers, whether it remains possible for a quorum of the approvers to approve the requested security change **(see, e.g., p. 13, paragraph [0049], FIG. 5A, element 514)**; and

- determining whether the requested security change is approved based on responses from the approvers to the approval request **(see, e.g. p. 13, paragraph [0049], FIG. 5A, elements 514, 516 and 518)**,

- the security change being used for determining access rights comprising permission to retrieve and to receive an electronic file from within a secure file store **(see, e.g., p. 7-8, paragraphs [0025], [0032] and [0033], FIG. 2, element 204)**.

D. Independent Claim 34

A method for approving a security change for a file security system that secures an electronic file **(see, e.g., p. 4, paragraph [0012], FIG. 3)**, comprising:

- receiving, in a computing device, **(see, e.g., p. 17, paragraph [0066])** a security change request from a requestor **(see, e.g., p. 9, paragraph [0036], FIG. 3, element 302)**, the security change being used for determining access rights comprising permission to retrieve and to receive the electronic file from within a secure file store **(see, e.g., p. 7-8, paragraphs [0032] and [0033], FIG. 2, element 204)**;

- determining whether the requestor is authorized to perform the requested security change **(see, e.g. p. 10, paragraph [0039], FIG. 4, element 404)**;

- receiving an approval request from the requestor **(see, e.g. p. 10, paragraph [0040], FIG. 4, element 406)**;

- based on the receipt of the approval request, performing at least the following:

    - identifying one or more approvers to approve or disapprove of the requested security change **(see, e.g. p. 11, paragraph [0042], FIG. 4, element 412)**;

- notifying the one or more approvers of an approval request for the requested security change **(see, e.g. p. 11, paragraph [0042], FIG. 4, element 412)**;

- determining, for at least one response received from the approvers, whether it remains possible for a quorum of the one or more approvers to approve the requested security change **(see, e.g., p. 13, paragraph [0049], FIG. 5A, element 514)**; and

- determining whether the requested security change is approved based on responses from the one or more approvers to the approval request **(see, e.g. p. 13, paragraph [0049], FIG. 5A, elements 514, 516 and 518)**.

E. Independent Claim 35

Claim 35 recites a file security system configured to restrict access to a secured electronic document **(see, e.g. p. 7-8, paragraph [0032], FIG. 2, element 200)**, comprising:

* an access server device configured to restrict access to the secured electronic document **(see, e.g., p. 8, paragraph [0032], FIG. 2, element 202)**; and

* an approval manager module operatively connected to said access server, wherein said approval manager module is configured to determine whether a security change is authorized **(see, e.g., p. 8, paragraph [0033], FIG. 2, element 208)**, the security change being used for determining permission to retrieve and to receive the secured electronic document from within a secure file store **(see, e.g., p. 8, paragraph [0033], FIG. 2, element 204)**, and wherein the approval manager module is configured to operate, in response to a determination that the security change is not authorized, a security change approval process upon receipt of an approval request to determine whether the security change is approved **(see, e.g. p. 11, paragraph [0042], FIG. 4, element 412)**,

* wherein the approval manager is further configured to determine, for at least one response received from the approvers, whether it remains possible for a quorum of approvers identified by the security change approval process to approve the requested security change **(see, e.g., p. 13, paragraph [0049], FIG. 5A, element 514)**.

F. Independent Claim 36

Claim 36 recites an article of manufacture including a computer-readable storage medium having stored thereon computer-executable instructions, execution of which, by a computing device, **(see, e.g., p. 17, paragraph [0066])** causes the computing device to perform operations for approving a security change for a file security system that secures an electronic file **(see, e.g., p. 4, paragraph [0012], FIG. 3)**, the operations comprising:

- determining whether the requested security change is authorized **(see, e.g. p. 10, paragraph [0039], FIG. 4, element 404)**, the security change being used for determining access rights comprising permission to retrieve and to receive the electronic file from within a secure file store **(see, e.g., p. 7-8, paragraphs [0032] and [0033], FIG. 2, element 204)**;

- notifying one or more approvers of an approval request for the requested security change in response to determining that the requested security change is not authorized **(see, e.g. p. 11, paragraph [0042], FIG. 4, element 412)**, and in response to receiving the approval request;

- determining, for at least one response received from the approvers, whether it remains possible for a quorum of the approvers to approve the requested security change **(see, e.g., p. 13, paragraph [0049], FIG. 5A, element 514)**; and

- determining whether the requested security change is approved based on responses from the one or more approvers to the approval **(see, e.g. p. 13, paragraph [0049], FIG. 5A, elements 514, 516 and 518)**.

G. Independent Claim 49

Claim 49 recites a method comprising:

- requesting a response from a plurality of approvers regarding a requested change of access rights to an electronic file **(see, e.g. see, e.g., p. 7-8, paragraphs [0032] and [0033], p. 11, paragraph [0042], FIG. 4, element 412)**;

- determining, for at least one response received from the approvers, whether it remains possible for a quorum of the approvers to approve the requested security change **(see, e.g., p. 13, paragraph [0049], FIG. 5A, element 514)**; and

- modifying, by a computing device, **(see, e.g., p. 17, paragraph [0066])** the access rights to the electronic file subject to approval of the requested security change based on responses from the plurality of approvers **(see, e.g., p. 13, paragraphs [0033] and [0051], FIG. 5A and 5B, element 518 and 528)**.

H. Independent Claim 50

Claim 50 recites an article of manufacture including a computer-readable storage medium having stored thereon computer-executable instructions, execution of which, by a computing device, **(see, e.g., p. 17, paragraph [0066])** causes the computing device to perform operations comprising:

- requesting a response from a plurality of approvers regarding a requested change of access rights to an electronic file **(see, e.g. see, e.g., p. 7-8, paragraphs [0032] and [0033], p. 11, paragraph [0042], FIG. 4, element 412)**;
- determining, for at least one response received from the approvers, whether it remains possible for a quorum of the approvers to approve the requested security change **(see, e.g., p. 13, paragraph [0049], FIG. 5A, element 514)**; and
- modifying the access rights to the electronic file subject to approval of the requested security change based on responses from the plurality of approvers **(see, e.g., p. 13, paragraphs [0033] and [0051], FIG. 5A and 5B, element 518 and 528)**.

I. Independent Claim 51

Claim 51 recites a file security system **(see, e.g. p. 7-8, paragraph [0032], FIG. 2, element 200)** comprising:

- an access server device configured to restrict access to an electronic file **(see, e.g., p. 8, paragraph [0032], FIG. 2, element 202)**; and
- an approval manager module operatively connected to the access server device **(see, e.g., p. 8, paragraph [0033], FIG. 2, element 208)** and configured to request a response from a plurality of approvers regarding a requested change of access rights to an electronic file **(see, e.g. see, e.g., p. 7-8, paragraphs [0032] and [0033], p. 11, paragraph [0042], FIG. 4, element 412)**, determine for at least one response received from the approvers whether it remains possible for a quorum of the approvers to approve the requested security change **(see, e.g., p. 13, paragraph [0049], FIG. 5A, element 514)**, and modify the access rights to the electronic file subject to approval of the requested security change based on responses from the plurality of approvers **(see, e.g., p. 13, paragraphs [0033] and [0051], FIG. 5A and 5B, element 518 and 528)**.

VI. Grounds of Rejection to be Reviewed on Appeal (37 C.F.R. § 41.37(c)(1)(vi))

A concise statement listing each ground of rejection presented for review follows.

A. Ground 1

Claims 1, 4, 15, 30, 37, 38, 45, 46 and 49-51 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,754,665 to Futagami *et al.* ("Futagami") in view of U.S. Patent Application Publication No. 2002/0156726 to Kleckner *et al.* ("Kleckner") and further in view of U.S. Patent Application Publication No. 2002/0062240 to Morinville ("Morinville").

B. Ground 2

Claims 2, 3, 5-14, 16, 18-29, 31-36, 47 and 48 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Futagami in view of Kleckner and Morinville and further in view of U.S. Patent No. 7,131,071 to Gune et *al.* ("Gune").

VII. Argument (37 C.F.R. § 41.37(c)(1)(vii))

There are two separate grounds of rejection to be reviewed on appeal.

A. Claims 1, 4, 15, 30, 37, 38, 45, 46 and 49-51 are not unpatentable under 35 U.S.C. § 103(a) over Futagami, Kleckner and Morinville

Independent Claims 1, 15, 30 and 49-51

The Examiner has rejected claims 1, 4, 15, 30, 37, 38, 45, 46 and 49-51 under 35 U.S.C. § 103(a) as allegedly being unpatentable over U.S. Patent No. 6,754,665 to Futagami *et al.* ("Futagami") in view of U.S. Patent Application Publication No. 2002/0156726 to Kleckner *et al.* ("Kleckner") and further in view of U.S. Patent Application Publication No. 2002/0062240 to Morinville ("Morinville"). Appellant respectfully traverses.

Claim 1 recites a method for approving a security change for a file security system that secures electronic files, comprising:

> receiving a request for the security change from a requestor, the security change being used for determining access rights comprising permission to retrieve and to receive an electronic file from within a secure file store;
>
> identifying a plurality of approvers to approve or disapprove of the requested security change by accessing an approver set in an approval manager module;
>
> notifying the approvers of an approval request for the requested security to change;
>
> determining, for at least one response received from the approvers, whether it remains possible for a quorum of the approvers to approve the requested security change; and
>
> determining whether the requested security change is approved based on responses from the approvers to the approval request.

As discussed in the Reply to Office Action 4 under 37 C.F.R. § 1.111 filed May 18, 2011, claim 1 recites *inter alia* "determining, for at least one response received from the

approvers, whether it remains possible for a quorum of the approvers to approve the requested security change." This language was the basis of the Examiner's allowance of September 29, 2010. (Notice of Allowability of September 29, 2010, p. 2 and 10). The Examiner has now reversed this earlier decision that the claims were in condition for allowance. On pages 2-3 of Final Office Action 4, the Examiner has noted that "...after reviewing the associated part of the specification relative to said feature, it was determined that, any system that stops the approval process once it is determined that one of the critical approvals have rejected the request, would disclose such feature. After further review of the prior art, it was determined that paragraph [0089] of Morinville (US Patent Application Publication No. 2002/0062240) teaches such scenario." The Examiner has not relied upon Futagami and Kleckner to teach these features.

On page 7 of Final Office Action 4, the Examiner noted that "Fu[tagami] and Kleckner are also analogous art, as they are both directed to system for controlling access to information. At the time of invention it would have been obvious to implement the approval process of Kleckner in view of Morinville in the system of Fu[tagami], which manages permissions for providing personal information. The motivation would have been to improve the change inquiry process of Fu[tagami] such that permission is allowed when a group of approvers approve the change request. This way a user may rely on approvers' expertise to decide if he/she should allow access to his/her personal information."

On page 17 of the Reply to Office Action 4, Appellant argued that "in Morinville, ***even if*** a quorum of approvers have approved a request, the request would nevertheless be denied if a single one of the 'necessary approvers' declines the request. (Morinville, paras.

[0088]-[0089])." In addition, on page 17 of the Reply to Office Action 4, Appellant provided a footnote: "Morinville does not operate on a quorum mechanism as claimed, and this is used simply to illustrate how Morinville could decline a request, even if quorum were reached, *arguendo*, using a mechanism ***other than*** quorum."

M.P.E.P. § 2142 notes that "[t]o reach a proper determination under 35 U.S.C. § 103, the examiner must step backward in time and into the shoes worn by the hypothetical 'person of ordinary skill in the art' when the invention was unknown and just before it was made. In view of all factual information, the examiner must then make a determination whether the claimed invention 'as a whole' would have been obvious at that time to that person. **Knowledge of applicant's disclosure must be put aside in reaching this determination**, yet kept in mind in order to determine the "differences," conduct the search and evaluate the "subject matter as a whole" of the invention. The tendency to resort to 'hindsight' based upon applicant's disclosure is often difficult to avoid due to the very nature of the examination process. **However, impermissible hindsight must be avoided and the legal conclusion must be reached on the basis of the facts gleaned from the prior art.**" (Emphasis Supplied).

Furthermore, according to M.P.E.P. § 2111, it is known that "the pending claims must be 'given their broadest reasonable interpretation consistent with the specification.'" *Phillips v. AWH Corp.*, 415 F.3d 1303, 75 USPQ2d 1321 (Fed. Cir. 2005).

Here, Morinville fails to teach "determining, for at least one response received from the approvers, ***whether it remains possible for a quorum of the approvers to approve the requested security change***." In fact, Morinville fails to teach or refer to "a quorum of the

approvers" and has completely taken the teachings of paragraph [0089] of Morinville out of the context of Morinville. Paragraph [0089] of Morinville merely teaches that "[t]he approval process is complete when either all of the approvers have approved the request, or one of the necessary approvers has declined the request." In fact, Morinville is silent regarding "a quorum of the approvers." The Examiner has improperly interpreted "the approval process is complete...when one of the necessary approvers has declined the request" as teaching "determining, for at least one response received from the approvers, whether it remains possible for a quorum of the approvers to approve the requested security change" by incorrectly reading "a quorum" into Morinville and falling victim to impermissible hindsight. Evidence of such is provided in the Examiner's rejection which includes the citation of Appellant's specification on page 7 of Office Action 4. There is no such teaching or suggestion of these features in Morinville as explained in the Reply to Office Action 4 on pages 17 and 18 and as elaborated upon in detail below. The actual teaching of paragraph [0089] of Morinville must be read in view of the rest of the disclosure in Morinville. Morinville describes the meaning of "one of the necessary approvers" and fails to refer to "a quorum of the approvers" as being necessary.

The Examiner has cited to portions of Morinville which describe "signature looping." This is described as "the process of identifying people within the company that are involved in a business process, notifying them that their participation is required for a particular process that has been initiated, and possibly obtaining their approvals of the process. (Morinville, [0013]). "Most competitive systems which are capable of automating signature looping do so by traversing the company's organizational structure directly up the chain of command as illustrated in FIG. 2. The customer defined the number of levels of

management that the business process requires and the system will automatically find the requester's superiors and forward information to them. These systems can identify the direct reporting manager, the second level manager and any other up to the CEO, but they cannot identify functional approvers like Finance or HR employees who are not directly above the requester in the organization." (Morinville, [0014]). "While some products allow signature looping to be based on the roles of employees rather than simply their positions, these products also normally require manual maintenance of lists which identify specific approvers for specific employees and specific business processes." (Morinville, [0016]).

Morinville describes its process for getting approval using automated signature looping as "the process of identifying people within the company that are involved in a business process and notifying them that their participation is required for a particular process that has been initiated. For example, if one employee requests the purchase of a certain item, it may be necessary for another employee to approve the purchase before it can proceed." (Morinville, [0067]). In addition, "[t]he purpose of automated signature looping is to identify the right participants in a business process (e.g., a request) without the need to manually maintain participant lists. The appropriate participants in the process can then view information associated with the process." (Morinville, [0068]). "If it is necessary to get approval from one management level for a business process, the direct reporting manager (who could hold the title of manager, director, etc. would be identified. This person could also be referred to as the first level manager. If two management levels are necessary for approval, the first level manager and the second level manager would be identified. The same process is used to identify however any levels of management are necessary." (Morinville, [0069]). The Examiner cited to paragraph [0089] of Morinville,

which notes that "[t]he approval process is complete when either all of the approvers have approved the request, or one of the necessary approvers has declined the request." (Morinville, [0089]). This process is illustrated in Figure 9 of Morinville provided below:

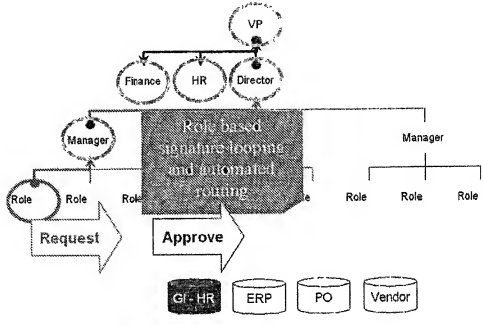

Fig. 9

Thus, Morinville teaches a hierarchical approval process for a business process that includes a request that is automatically routed up a hierarchical chain in an organization. Paragraph [0069] and [0089] support this interpretation: "[i]f two management levels are necessary for approval, the first level manager and the second level manager would be identified. The same process is used to identify however any levels of management are

necessary." It is clear that Morinville, in combination with Futagami and Kleckner, fails to teach or suggest "determining, for at least one response received from the approvers, whether it remains possible for a quorum of the approvers to approve the requested security change."

As a non-limiting example, and interpreting these features of claim 1 with the broadest reasonable interpretation consistent with the instant specification, paragraph [0049] indicates that "a quorum of the approvers" may be interpreted as more than 50% of the approvers.[1] Furthermore, claim 1 recites "a plurality of approvers," meaning that there must be more than one approver. Taking this view into consideration, we may look to Morinville to determine if Morinville teaches whether it is possible to determine for at least one response received from the approvers, whether it remains possible for a quorum of the approvers to approve the requested security change.

According to the teachings of Morinville, the only way that a business process may be approved is through unanimous approval by all necessary approvers. **Thus, it is never possible to determine whether a business process will be approved until all managers have provided their decision.** It does not matter if a quorum of managers agree with a business decision if a single manager rejects the business decision. According to the teachings of Morinville, if a first, second and third level manager's approval is necessary for approval, if the first manager rejects, then it does not matter if a quorum of the managers would agree to the business process because only one manager needs to reject the business

1 Page 13 of the instant specification provides that "if an approver set has five approvers and requires a quorum of three, then if responses from three approvers have already denied approval, then approval by a quorum of approvers is no longer possible." This was also quoted in Response to Office Action 4 on page 17.

process. In fact, the second and third managers are not even given an opportunity to approve. However, if the first manager approves, this provides an indeterminable result regarding the business decision. While it remains possible for a quorum of the approvers to agree with the business decision (first and second manager), the first and second manager cannot approve the business decision without unanimous agreement. If the third manager rejects the business decision, then even if a quorum of the managers agree with the decision, it will be rejected. Thus, it is not possible to determine with the approval of one business manager, whether a quorum of business managers approve the business decision, because an approval must be unanimous. Thus, Morinville does not teach determining whether it remains possible for a quorum of the approvers to approve the requested security change if one approval or rejection is provided.

It is known that "[a] prior art reference must be considered in its entirety, i.e., as a whole, including portions that would lead away from the claimed invention." (M.P.E.P. § 2141.02 & *W.L. Gore & Associates, Inc. v. Garlock, Inc.*, 721 F.2d 1540, 220 USPQ 303 (Fed. Cir. 1983), *cert. denied*, 469 U.S. 851 (1984)).

It is submitted that one of ordinary skill in the art at the time of the invention would not have been motivated to combine the teachings of Morinville with the teachings of Kleckner and Futagami. As described above, it does not matter if a quorum of business managers agree with a business process. Morinville discloses that a business process is approved only through unanimous approval and that if any of the necessary business managers reject the business process, that it may not be approved. In Morinville, there is no reason to keep track or determine if a quorum of the business managers approve a decision

because this does not matter. Either all approve, or the business decision is rejected. Thus, because **it is never possible to determine whether a business process will be approved until all managers have provided their decision**, it is submitted that Futagami, Kleckner and Morinville do not render the features of claim 1 obvious because Morinville teaches away from "determining, for at least one response received from the approvers, whether it remains possible for a quorum of the approvers to approve the requested security change."

The Supreme Court has indicated that an Examiner should not be denied recourse to use common sense in rejecting claims under 35 U.S.C. § 103(a) based on obviousness, but in this case, common sense would have motivated an ordinary person in the art at the time of the invention to discount the teachings of Morinville. *KSR International Co. v. Teleflex Inc. (KSR)*, 550 U.S. 398, 82 USPQ2d 1385, 1395 (2007). As noted above, Morinville explicitly discloses that **all** business managers must approve a business decision and that if a single manager rejects a decision, then it is rejected. Thus, because there is no teaching of and no reason to determine whether it remains possible for a quorum of the business managers to approve a business decision in Morinville, and because these features are also not taught by Futagami or Kleckner, the features of claim 1 would not have been obvious.

For at least the aforementioned reasons, claim 1 is not obvious in view of Futagami, Kleckner and Morinville. Claims 4, 37, 38 and 45 depend from claim 1, and are likewise not obvious for at least the same reasons as claim 1, and further in view of their own respective features.

Independent claims 15, 30 and 49-51 distinguish over Futagami, Kleckner and Morinville for at least the same reasons provided with regard to claim 1, and further in view

of their own respective features. Dependent claim 46 depends from claim 30 and is likewise not obvious for at least the same reasons as claim 30, and further in view of its own respective features.

Accordingly, Appellant respectfully requests that that the rejection of claims 1, 4, 15, 30, 37, 38, 45, 46 and 49-51 under 35 U.S.C. § 103(a) be reversed.

B. Claims 2, 3, 5-14, 16, 18-29, 31-36, 47 and 48 are not unpatentable under 35 U.S.C. § 103(a) over Futagami, Kleckner, Morinville and Gune

Independent Claims 34-36

Independent claim 34 recites *inter alia* "determining, for at least one response received from the approvers, whether it remains possible for a quorum of the one or more approvers to approve the requested security change." Similar distinguishing features are recited in independent claims 35 and 36. For reasons similar to those noted above with regard to claim 1, the combination of Futagami, Kleckner and Morinville fails to teach or suggest at least these features of claims 34-36. Gune does not supply the missing teaching or suggestion, nor does the Examiner rely on Gune as allegedly supplying the missing teaching or suggestion. Accordingly, independent claims 34-36 are not obvious in view of Futagami, Kleckner, Morinville and Gune.

Dependent claims 2, 3, 5-14, 16, 18-29, 31-33, 47 and 48 depend from the above discussed independent claims and are likewise not obvious for at least the same reasons and further in view of their own respective features.

In addition, dependent claim 29 independently distinguishes over Futagami, Kleckner, Morinville and Gune. Claim 29 recites "a key store operatively connected to said

access server and configured to store cryptographic keys used to gain access to the secured electronic documents." On page 12 of Final Office Action 4, the Examiner noted that "[w]ith regards to claims 20 and 29, a key store connected to the system that uses digital signatures is inherent to systems using digital signature because keys are integral parts of digital signatures." The Examiner has not relied upon any of the applied references. No other details or reasons are provided for the rejection.

The Examiner has failed to refer to any of the applied references, thus, this appears to be a rejection based on Official Notice. M.P.E.P. § 2144.03 notes that "[o]fficial notice without documentary evidence to support an examiner's conclusion is permissible only in some circumstances. While 'official notice' may be relied on, these circumstances should be rare when an application is under final rejection or action under 37 CFR 1.113. Official notice unsupported by documentary evidence should only be taken by the examiner where the facts asserted to be well-known, or to be common knowledge in the art are capable of instant and unquestionable demonstration as being well-known." The Examiner has failed to demonstrate that "the facts asserted to be well-known, or to be common knowledge in the art are capable of instant and unquestionable demonstration as being well-known." Appellant submits "a key store" as recited in claim 29 that is connected to the access server, as shown in Figure 2 of the specification would not have merely been common knowledge.

Furthermore, it has been held that "[i]t is never appropriate to rely solely on 'common knowledge' in the art without evidentiary support in the record, as the principal evidence upon which a rejection was based." *In re Zurko*, 258 F.3d 1379, 1385, 59 USPQ2d 1693, 1697 (Fed. Cir. 2001). Because the Examiner has failed to establish that features are

common knowledge or well-known and has failed to provide evidentiary support, the rejection is improper and should be reversed.

Appellant respectfully requests that that the rejection of claims 2, 3, 5-14, 16, 18-29, 31-36, 47 and 48 under 35 U.S.C. § 103(a) be reversed.

C. Conclusion

For at least the aforementioned reasons, the Examiner's rejections of claims 1-16, 18-38 and 45-51 under 35 U.S.C. § 103 are improper. Therefore, Appellant respectfully requests that the Board reverse the Examiner's final rejection of these claims, and remand this application for allowance of claims 1-16, 18-38 and 45-51.

Respectfully submitted,

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.

Glenn J. Perry
Attorney for Applicant
Registration No. 28,458

Date: 5 Oct. 2011

1100 New York Avenue, N.W.
Washington, D.C. 20005-3934
(202) 371-2600

VIII. Claims Appendix

1. (Previously Presented) A method for approving a security change for a file security system that secures electronic files, comprising:

receiving a request for the security change from a requestor, the security change being used for determining access rights comprising permission to retrieve and to receive an electronic file from within a secure file store;

identifying a plurality of approvers to approve or disapprove of the requested security change by accessing an approver set in an approval manager module;

notifying the approvers of an approval request for the requested security to change;

determining, for at least one response received from the approvers, whether it remains possible for a quorum of the approvers to approve the requested security change; and

determining whether the requested security change is approved based on responses from the approvers to the approval request.

2. (Previously Presented) The method as recited in claim 1, wherein said notifying of the approvers is achieved by electronic mail.

3. (Previously Presented) The method as recited in claim 2, further comprising:

receiving the responses from the approval group as electronic mail.

4. (Previously Presented) The method as recited in claim 1, wherein determining whether the requested security change is approved includes determining that no one of the plurality of approvers is authorized to individually approve the requested security change.

5. (Previously Presented) The method as recited in claim 1, wherein identifying the plurality of approvers comprises:

identifying a plurality of approvers that are arranged as a set or group.

6. (Previously Presented) The method as recited in claim 1, wherein identifying the plurality of approvers comprises:

identifying a plurality of approvers that are arranged in a plurality of sets or groups, wherein said determining whether the requested security change is approved comprises evaluating whether more than one of the plurality of sets or groups have approved the requested security change.

7. (Previously Presented) The method as recited in claim 6, wherein identifying the plurality of approvers comprises:

identifying a plurality of sets or groups that are arranged in a hierarchy, and wherein progression to a next level in the hierarchy comprises obtaining approval from the set or group associated with a current level.

8. (Previously Presented) The method as recited in claim 1, wherein identifying the plurality of approvers comprises:

identifying a plurality of users of the file security system.

9. (Previously Presented) The method as recited in claim 1, wherein identifying the plurality of approvers comprises:

identifying a plurality of approvers that form a set of approvers, wherein said determining whether the requested security change is approved comprises evaluating whether a subset of the set of approvers approve the requested security change.

10. (Previously Presented) The method as recited in claim 1, wherein identifying the plurality of approvers comprises:

identifying the approvers based on the requested security change.

11. (Previously Presented) The method as recited in claim 1, wherein identifying the plurality of approvers comprises:

identifying the approvers based on the requestor.

12. (Previously Presented) The method as recited in claim 1, wherein said notifying operates to substantially simultaneously notify all of the approvers of the approval request for the requested security change.

13. (Previously Presented) The method as recited in claim 1, wherein said notifying operates to substantially concurrently notify all of the approvers of the approval request for the requested security change.

14. (Previously Presented) The method as recited in claim 1, wherein receiving the request for the security change comprises:

receiving a request for a security change that applies to electronic documents.

15. (Previously Presented) A file security system configured to restrict access to secured electronic documents, comprising:

an access server device configured to restrict access to the secured electronic documents; and

an approval manager operatively connected to said access server and configured to operate a security change approval process to determine whether a requested security change is approved, the security change being used for determining access rights comprising permission to retrieve and to receive the secured electronic documents from within a secure file store,

wherein, in operating the security change approval process, the approval manager is configured to notify a plurality of approvers of the requested security change, to ask the approvers to approve or disapprove the requested security change, and to access an approver set to identify the plurality of approvers, and

wherein the approval manager is further configured to determine, for at least one response received from the approvers, whether it remains possible for a quorum of the approvers to approve the requested security change.

16. (Previously Presented) The file security system as recited in claim 15, wherein said approval manager is configured to operate the security change approval process without any interaction from a system administrator.

17. (Cancelled)

18. (Previously Presented) The file security system as recited in claim 15, wherein the approval manager is configured to notify the approvers of the requested security change by electronic mail messages.

19. (Previously Presented) The file security system as recited in claim 18, wherein the approval manager is configured to enable the approvers to approve or disapprove the requested security change using reply electronic mail messages.

20. (Previously Presented) The file security system as recited in claim 19, wherein the approval manager is configured to enable the approvers to reply to the requested security change by electronic mail messages that include a digital signature of the associated approver to verify authenticity.

21. (Previously Presented) The file security system as recited in claim 15, wherein the approval manager is configured to specify that no one of the approvers is permitted to individually approve the requested security change.

22. (Previously Presented) The file security system as recited in claim 15, wherein the approval manager is configured to arrange the approvers as a set or group.

23. (Previously Presented) The file security system as recited in claim 15, wherein the approval manager is configured to arrange the approvers into a plurality of sets or groups, and

wherein said approval manager is configured to obtain approval from more than one of the plurality of sets or groups in order to determine that the requested security change is approved.

24. (Previously Presented) The file security system as recited in claim 23, wherein the approval manager is configured to arrange the plurality of sets or groups of approvers in a hierarchy, and wherein the approval manager is configured to allow progression of at least one of the approvers to a next level in the hierarchy in response to approval of the at least one approver from the set or group of approvers associated with a current level.

25. (Previously Presented) The file security system as recited in claim 15, wherein the approvers are users of the file security system.

26. (Previously Presented) The file security system as recited in claim 15, wherein the plurality of approvers form a set of approvers, and

wherein said approval manager is configured to determine that the requested security change is approved in response to a subset of the set of approvers approving the requested security change.

27. (Previously Presented) The file security system as recited in claim 15, wherein said approval manager is configured to identify the plurality of approvers dependent on the requested security change.

28. (Previously Presented) The file security system as recited in claim 15, wherein said approval manager is configured to identify the plurality of approvers dependent on the requestor.

29. (Previously Presented) The file security system as recited in claim 15, further comprising:

a key store operatively connected to said access server and configured to store cryptographic keys used to gain access to the secured electronic documents.

30. (Previously Presented) An article of manufacture including a computer-readable storage medium having stored thereon computer-executable instructions, execution of which, by a computing device, causes the computing device to perform operations for approving a security change for a file security system that secures electronic files, the operations comprising:

notifying a plurality of approvers of an approval request for the requested security change, the plurality of approvers identified by accessing an approver set in an approval manager module;

determining, for at least one response received from the approvers, whether it remains possible for a quorum of the approvers to approve the requested security change; and

determining whether the requested security change is approved based on responses from the approvers to the approval request,

the security change being used for determining access rights comprising permission to retrieve and to receive an electronic file from within a secure file store.

31. (Previously Presented) The article of manufacture as recited in claim 30, wherein said notifying of the approvers is achieved by electronic mail.

32. (Previously Presented) The article of manufacture as recited in claim 31, wherein the responses from the approval group are electronic mail.

33. (Previously Presented) The article of manufacture as recited in claim 30, wherein no one of the plurality of approvers can individually approve the requested security change.

34. (Previously Presented) A method for approving a security change for a file security system that secures an electronic file, comprising:

receiving, in a computing device, a security change request from a requestor, the security change being used for determining access rights comprising permission to retrieve and to receive the electronic file from within a secure file store;

determining whether the requestor is authorized to perform the requested security change;

receiving an approval request from the requestor;

based on the receipt of the approval request, performing at least the following:

identifying one or more approvers to approve or disapprove of the requested security change;

notifying the one or more approvers of an approval request for the requested security change;

determining, for at least one response received from the approvers, whether it remains possible for a quorum of the one or more approvers to approve the requested security change; and

determining whether the requested security change is approved based on responses from the one or more approvers to the approval request.

35. (Previously Presented) A file security system configured to restrict access to a secured electronic document, comprising:

an access server device configured to restrict access to the secured electronic document; and

an approval manager module operatively connected to said access server, wherein said approval manager module is configured to determine whether a security change is authorized, the security change being used for determining permission to retrieve and to receive the secured electronic document from within a secure file store, and wherein the approval manager module is configured to operate, in response to a determination that the security change is not authorized, a security change approval process upon receipt of an approval request to determine whether the security change is approved,

wherein the approval manager is further configured to determine, for at least one response received from the approvers, whether it remains possible for a quorum of approvers identified by the security change approval process to approve the requested security change.

36. (Previously Presented) An article of manufacture including a computer-readable storage medium having stored thereon computer-executable instructions, execution of which, by a computing device, causes the computing device to perform operations for approving a security change for a file security system that secures an electronic file, the operations comprising:

determining whether the requested security change is authorized, the security change being used for determining access rights comprising permission to retrieve and to receive the electronic file from within a secure file store;

notifying one or more approvers of an approval request for the requested security change in response to determining that the requested security change is not authorized, and in response to receiving the approval request;

determining, for at least one response received from the approvers, whether it remains possible for a quorum of the approvers to approve the requested security change; and

determining whether the requested security change is approved based on responses from the one or more approvers to the approval.

37. (Previously Presented) The method of claim 1, wherein receiving the request for the security change comprises:

receiving a request that relates to a secure file store that is located at the file security system.

38. (Previously Presented) The method of claim 1, wherein receiving the request for the security change comprises:

receiving a request that relates to a secure file store that is located at the requestor.

39-44. (Cancelled)

45. (Previously Presented) The method of claim 1, further comprising:

performing the requested security change in response to determining that the requested security change has been approved.

46. (Previously Presented) The article of manufacture as recited in claim 30, the operations further comprising:

performing the requested security change when said determining determines that the requested security change has been approved.

47. (Previously Presented) The method of claim 34, further comprising:

performing the requested security change in response to determining that the requestor is authorized to perform the requested security change, or in response to determining that the requested security change has been approved.

48. (Previously Presented) The article of manufacture of claim 36, the operations further comprising:

performing the requested security change in response to determining that the requested security change is authorized, or in response to determining that the requested security change has been approved.

49. (Previously Presented) A method comprising:

requesting a response from a plurality of approvers regarding a requested change of access rights to an electronic file;

determining, for at least one response received from the approvers, whether it remains possible for a quorum of the approvers to approve the requested security change; and

modifying, by a computing device, the access rights to the electronic file subject to approval of the requested security change based on responses from the plurality of approvers.

50. (Previously Presented) An article of manufacture including a computer-readable storage medium having stored thereon computer-executable instructions, execution of which, by a computing device, causes the computing device to perform operations comprising:

requesting a response from a plurality of approvers regarding a requested change of access rights to an electronic file;

determining, for at least one response received from the approvers, whether it remains possible for a quorum of the approvers to approve the requested security change; and

modifying the access rights to the electronic file subject to approval of the requested security change based on responses from the plurality of approvers.

51. (Previously Presented) A file security system comprising:

an access server device configured to restrict access to an electronic file; and

an approval manager module operatively connected to the access server device and configured to request a response from a plurality of approvers regarding a requested change of access rights to an electronic file, determine for at least one response received from the approvers whether it remains possible for a quorum of the approvers to approve the requested security change, and modify the access rights to the electronic file subject to approval of the requested security change based on responses from the plurality of approvers.

IX. Evidence Appendix

To the best of the knowledge of Appellant, Appellant's legal representative, and Appellant's assignee, there has been no evidence submitted pursuant to 37 C.F.R. §§ 1.130, 1.131, or 1.132, nor has any other evidence been entered in the record by the Examiner and relied upon in this Appeal Brief.

X. Related Proceedings Appendix

Not applicable